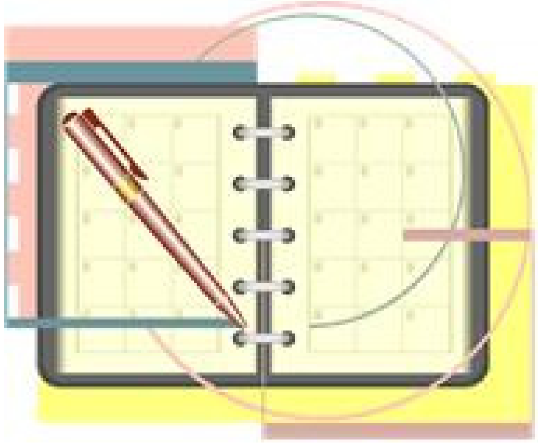
David K. Hemsath
Senior Technical Staff Member, IBM Security Solutions
CISSP, CISSP-ISSAP, CPHIMS, IEEE SM, ACM SM
dhemsath@us.ibm.com

Identity and Access Assurance Solution
Nebraska Cyber Security Conference
26 July 2011

Agenda

- What organizations care about
- Identity and access assurance (IAA) in the context of IBM’s security framework
- IAA details
  - Identity management
  - Authentication and authorization
  - User activity monitoring
- Special case: Privileged Identity Management (PIM)
- IAA design patterns



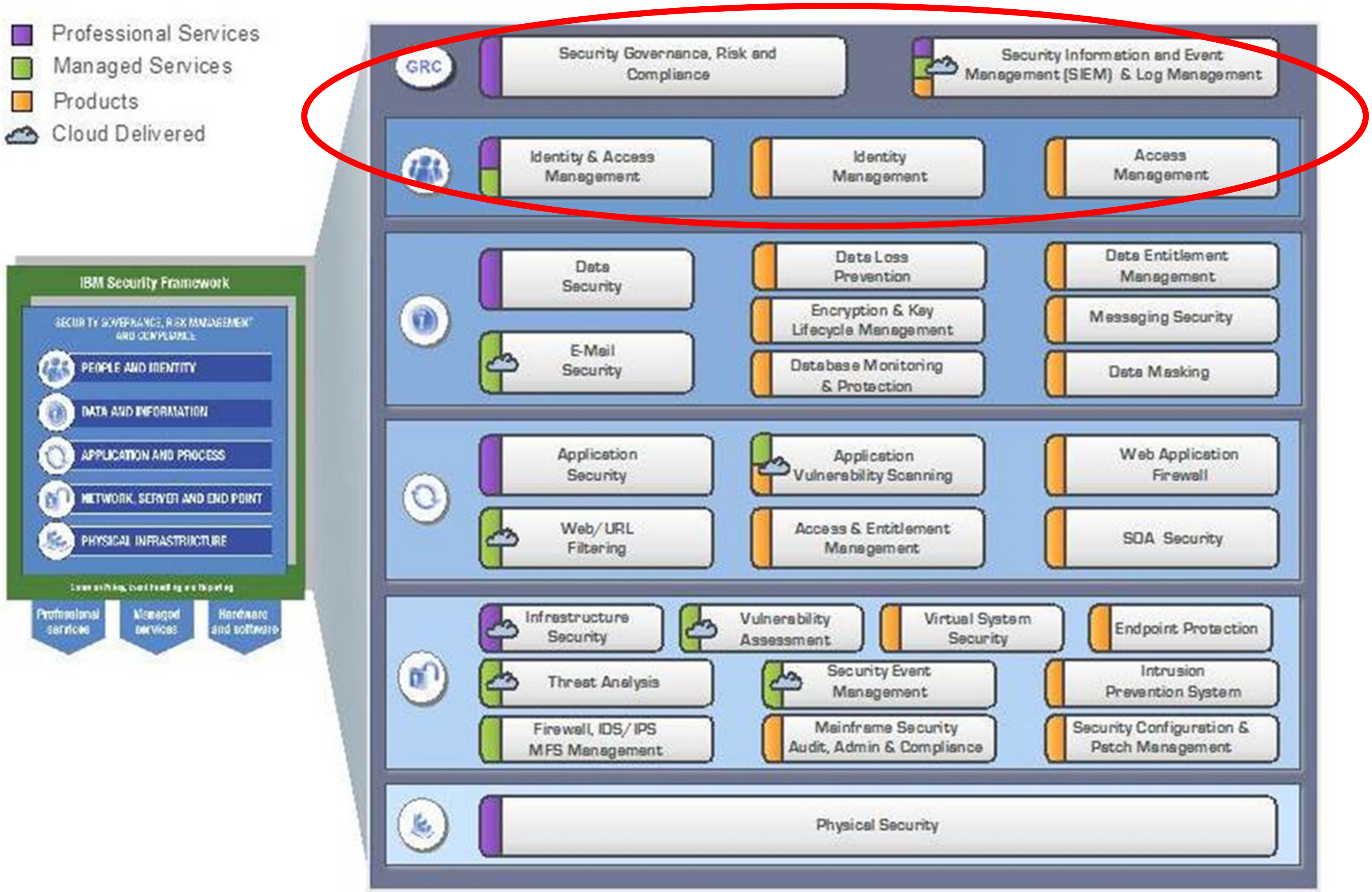
Fundamentally, organizations care about two things

- The continuity of their operations, and
- Protecting sensitive/critical information

Or, put another way, staying out of the news and staying out of court!

- To achieve this, organizations need to:
  1. Know **who** is coming into their systems,
  2. Know **what** they did, and
  3. Be able to **prove it** to their internal auditors and external regulators.

IBM’s security framework and solutions



🟪 Professional Services
🟩 Managed Services
🟧 Products
☁ Cloud Delivered

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Professional services

Managed services

Hardware and software

GRC

Security Governance, Risk and Compliance

Security Information and Event Management (SIEM) & Log Management

Identity & Access Management

Identity Management

Access Management

Data Security

Data Loss Prevention

Data Entitlement Management

Encryption & Key Lifecycle Management

Messaging Security

E-Mail Security

Database Monitoring & Protection

Data Masking

Application Security

Application Vulnerability Scanning

Web Application Firewall

Web/URL Filtering

Access & Entitlement Management

SOA Security

Infrastructure Security

Vulnerability Assessment

Virtual System Security

Endpoint Protection

Threat Analysis

Security Event Management

Intrusion Prevention System

Firewall, IDS/IPS MFS Management

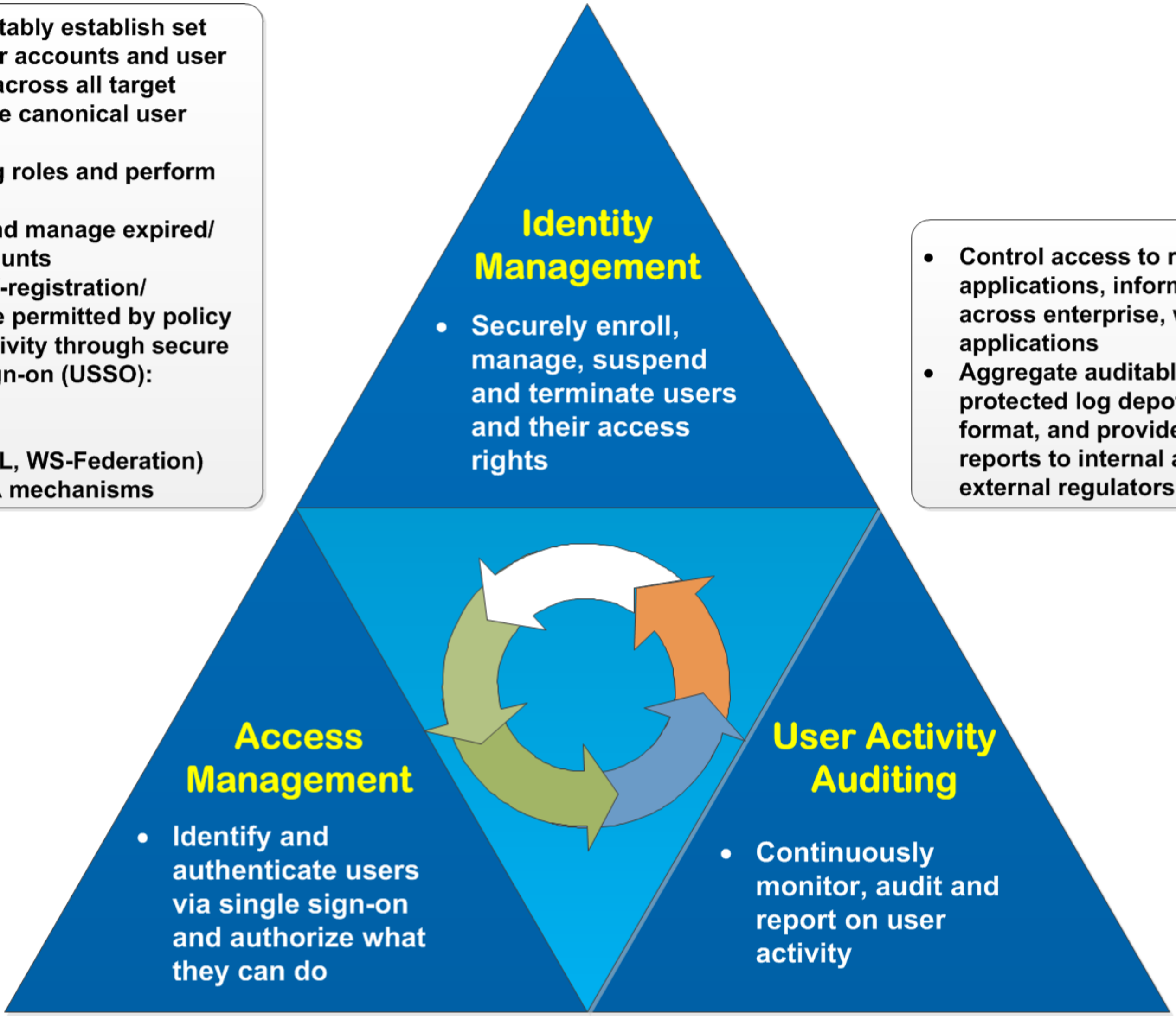
Mainframe Security Audit, Admin & Compliance

Security Configuration & Patch Management

Physical Security

Identity and access assurance

- Quickly and auditably establish set and recertify user accounts and user account access across all target systems from one canonical user definition
- Discover existing roles and perform role engineering
- Quickly locate and manage expired/ invalid user accounts
- Provide user self-registration/ enrollment where permitted by policy
- Increase productivity through secure unified single sign-on (USSO):
  * web
  * desktop
  * federated (SAML, WS-Federation)
  * multi-factor I&A mechanisms



Identity Management

- Securely enroll, manage, suspend and terminate users and their access rights

Access Management

- Identify and authenticate users via single sign-on and authorize what they can do

User Activity Auditing

- Continuously monitor, audit and report on user activity

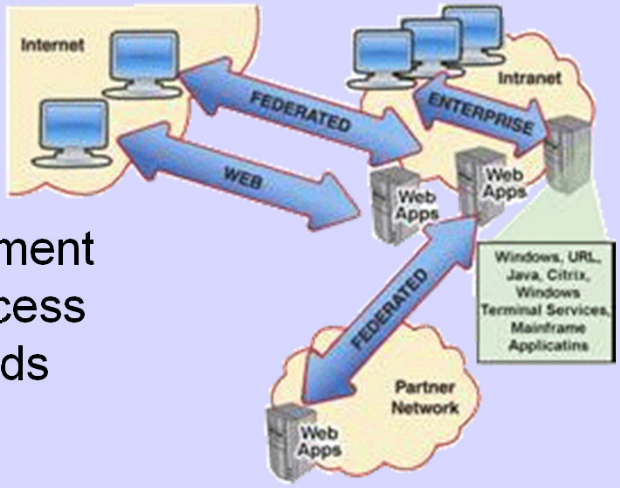
- Control access to resources (e.g., applications, information) consistently across enterprise, web and SOA-based applications
- Aggregate auditable events in a protected log depot, normalize into W7 format, and provide dashboards and reports to internal auditors and external regulators

Why Identity and access assurance?

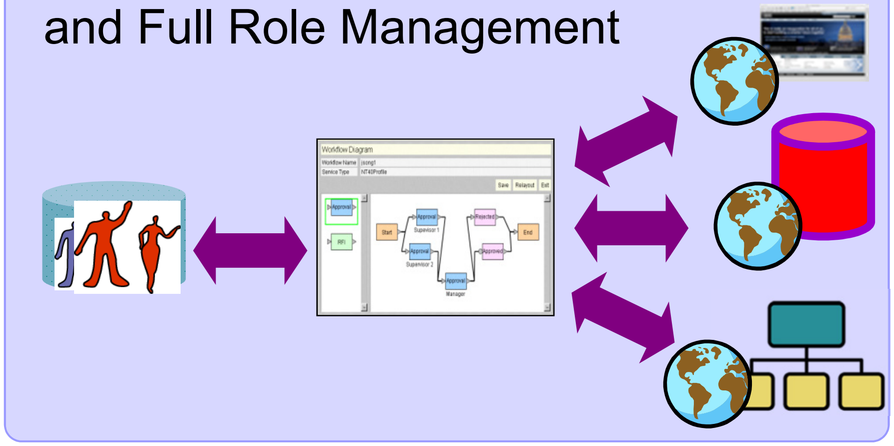
- Improve service
  - Common IT services portal can offer identity services
  - Enable collaboration via role-based portals with access to enterprise services and applications
  - Increase reach with federated models leveraging trusted identity information
- Reduce Cost
  - Reduce help desk costs, password resets
  - More efficiently manage restructuring
- Manage Risk
  - Privileged/shared IDs
  - Expired/invalid accounts
  - Prevent insider breach
  - Recertification, access attestation
  - Support for appropriate strength user credentials
  - Unauthorized privilege change detection

Pains addressed by identity and access assurance

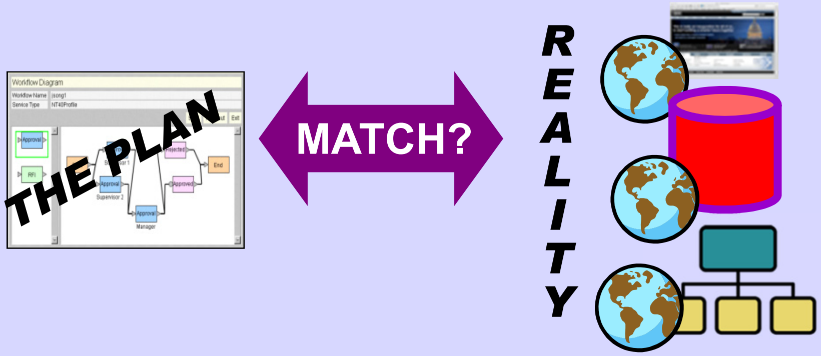
Single Sign On & Management of Web Access & Passwords



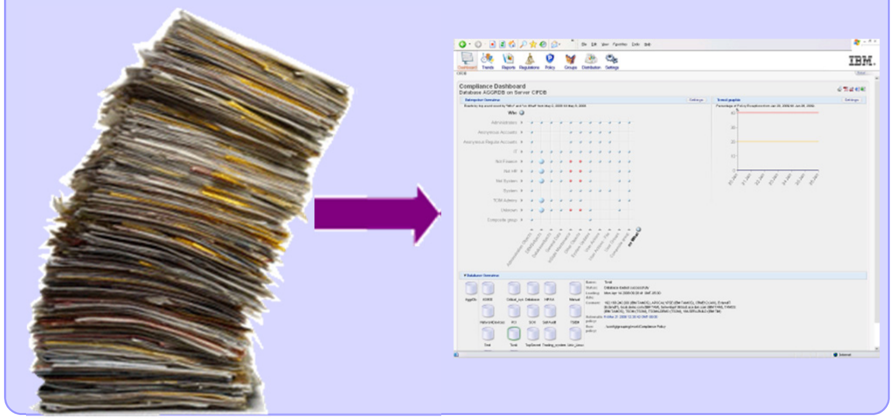
User Provisioning / Deprovisioning and Full Role Management



The 3 Rs – Reconciliation, Recertification & Reporting



Security log management & reporting



Privileged Identity Management

- What is a privileged identity?
  - Has access to sensitive resources
  - Required by virtually all platforms although modern platforms have more capabilities for separating PIM from general user access
    - Aside: “Least privilege” unaware developers
  - Often shared
  - Examples:
    - Root
    - Essential system processes that are over-privileged (a decreasing problem, but a reason that NIST SP 800-xxx guidance recommends only running required services, daemons, etc.)
    - Sysadmins/DBAs
    - Executives and their AAs
    - Oracle Financials Admin
    - SAP Admin

    …

Who cares about privileged users?
Your auditors/regulators do!

Compliance Initiative	Relation to Privileged Account Controls
Payment Card Industry (PCI) Data Security Standard (DSS)	Protect stored cardholder data (#3) Develop and maintain secure systems and applications (#6) Restrict access to cardholder data by business need-to-know (#7) Insufficient internal controls over privileged accounts would negatively impact an organization's capability to meet all of these requirements.
California Senate Bill 1386 (now California Civil Code 1798) Other State Privacy Regulations	SB 1386 requires organizations that lose private information of California residents to report the loss to affected individuals. Unauthorized users of privileged accounts can bypass the access control mechanisms and audit controls of most systems to access private information without the organization knowing about it.
Sarbanes-Oxley Act (SOX) Section 404	Requires corporate management to take responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting Requires management to assess and report the effectiveness of the internal control structure and procedures for financial reporting. Insufficient internal controls over privileged accounts negatively impact an organization's capability to meet these requirements.
EU Data Protection Act	Appropriate technical measures must be taken against unlawful processing of Personal data and against accidental loss .. Including controlling access to info Insufficient internal controls over privileged accounts negatively impact an organization's capability to meet these requirements

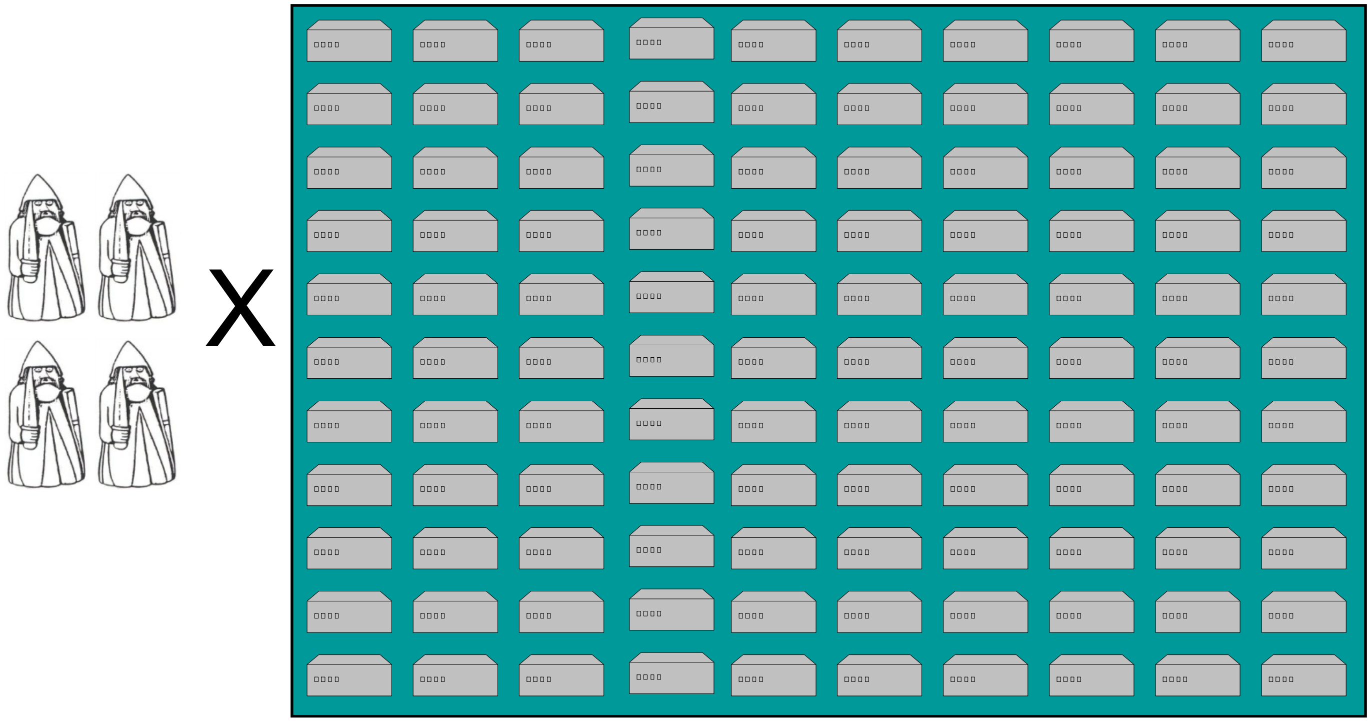
Problem Statement – Illustration (1)

The ‘Standard’ identity management model leads to an exponential increase in the number of privileged userids, and exponential increase in cost and risk

Originally, small teams ran servers locally

4 administrators

100 servers



= 400 Admin IDs

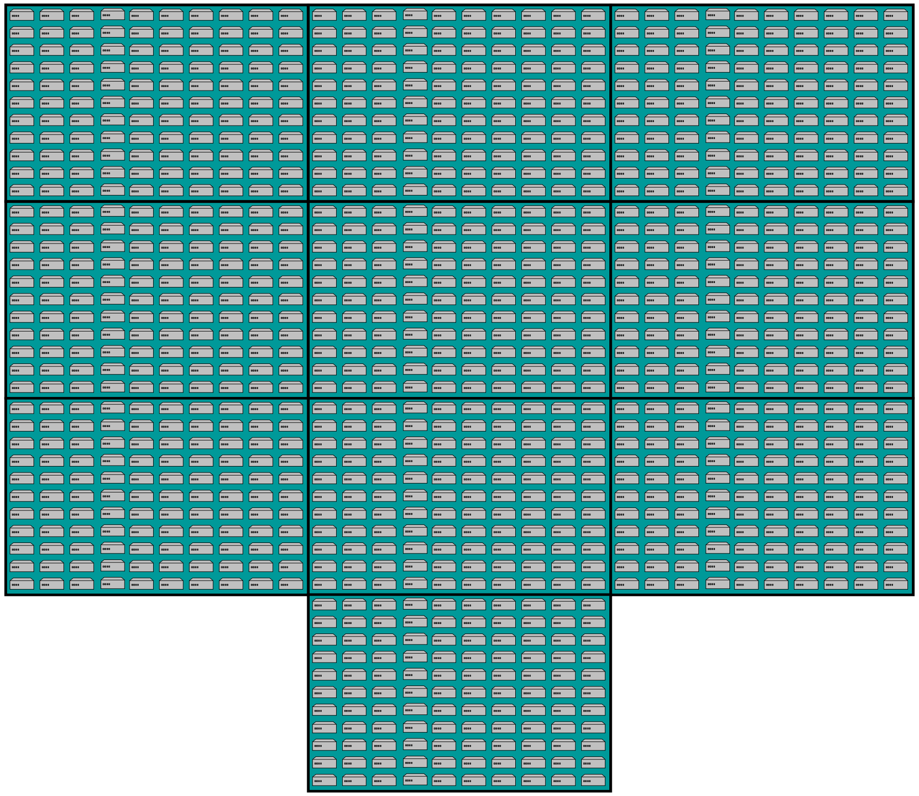
Problem Statement – Illustration (2)

Then we developed Data Centers

40 administrators

X

1000 servers



= 40,000 Admin IDs

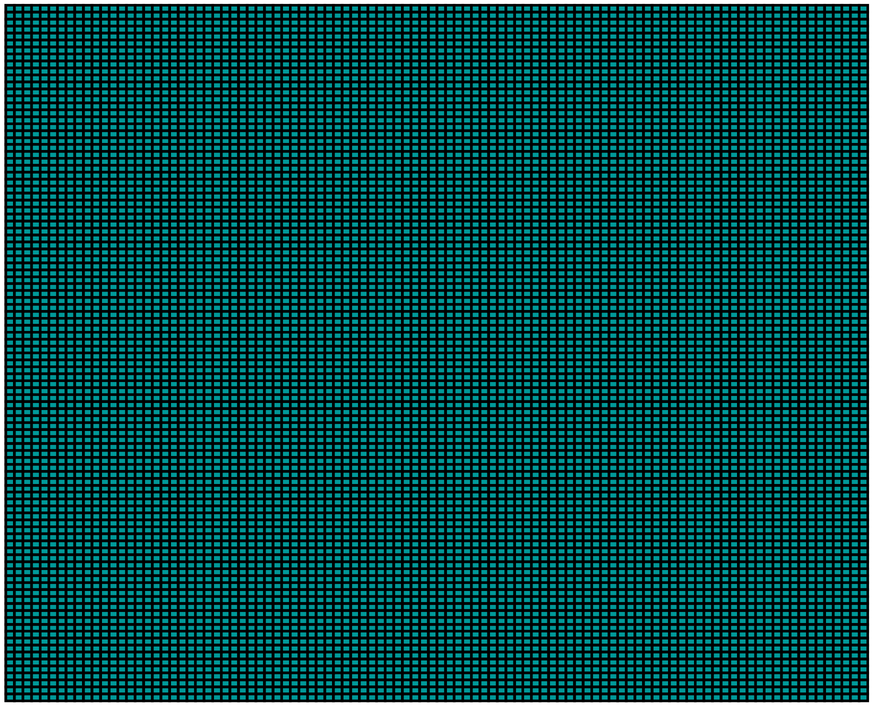
Problem Statement – Illustration (3)

Then we developed Global Delivery Centers

400 administrators

X

10000 servers



= 4 million Admin IDs

Problem Statement

The traditional approach requires EITHER:

- Each administrator to have a userid on every system they administer
  - Exponential increase in privileged userids
  - Increased risk of mismanagement of privileged userids
  - Increased userid administration costs

OR

- Administrators share privileged userids
  - Risk of losing ‘accountability’
  - Issues with password management and security
  - Out of step with regulatory thinking
- The proliferation of Virtualization, Data Centers, Cloud Computing and fine grained Roles/Entitlement management will greatly exacerbate this problem
- Privilege Identity Management combines the best features of both approaches, without the disadvantages

Known People (un)Intentionally Do Great Harm

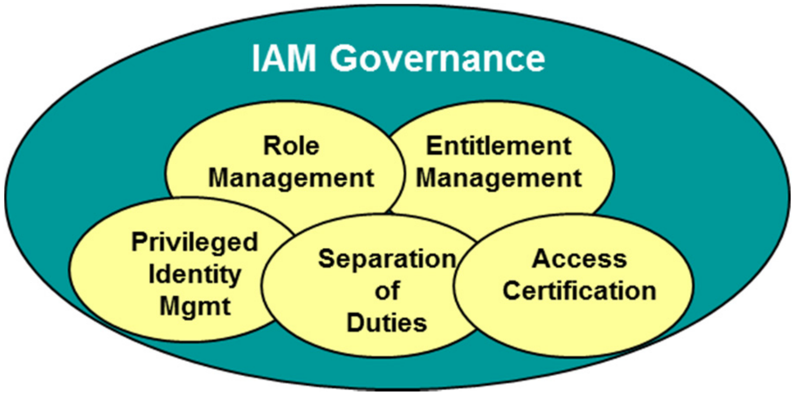
- **Known people with privileged identities unintentionally or intentionally do harm**
  - eCrime survey, 2007-2009 average – over 50% of respondents experienced at least 1 malicious insider incident
  - IT sabotage/theft for business advantage are generally committed by technical, privileged users
  - Insider attacks are often more costly than attacks coming from external sources
  - CERT best practice guidelines recommend “Use extra caution with system admin, technical or privileged users”

Sources:

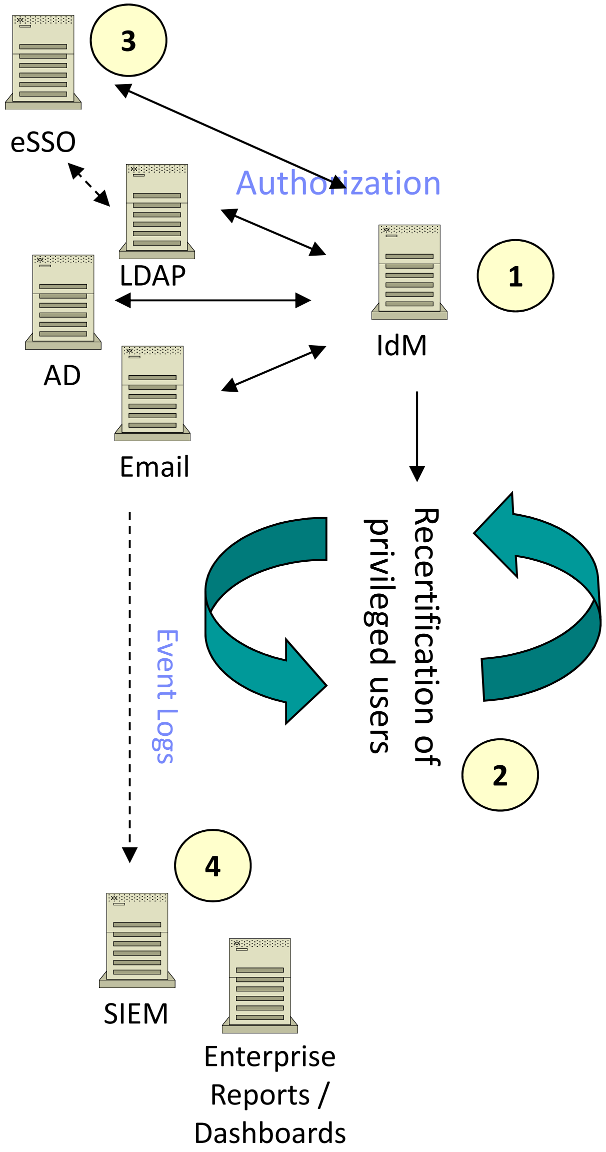
- 2010 Cybersecurity (e-crime) Watch Survey (conducted by CSO, the U.S. Secret Service, CERT and Deloitte's Center for Security & Privacy Solutions)
- Ponemon Institute's Cost of Cyber Crime Study 2010
- “Common sense guide to detection and prevention of insider threats” 3rd edition - v3.1, CERT, Jan 09

Privileged Identity Management is an integral part of IAM Governance

- Key PIM functions include:
  - Centralized management of privileged and shared identities
  - Secure access and storage of shared identities
  - Single sign-on with automated check in and check out of shared and privileged IDs
  - End to end monitoring and reporting
- Benefits
  - Centralized Privileged ID management improves IT control and **reduces risk**
  - Automated sign on and check-in/out simplifies usage and **reduces cost**
  - Comprehensive tracking and reporting **enhances accountability and compliance**



How it works



3
eSSO
Authorization
LDAP
AD
Email
1
IdM
Recertification of privileged users
2
Event Logs
4
SIEM
Enterprise Reports / Dashboards

1

- IdM with extensions provisions privileged IDs and manages pools of shared IDs
- Shared IDs are stored in a secured data store

2

- Periodically recertify account authorizations through a consistent work flow.

3

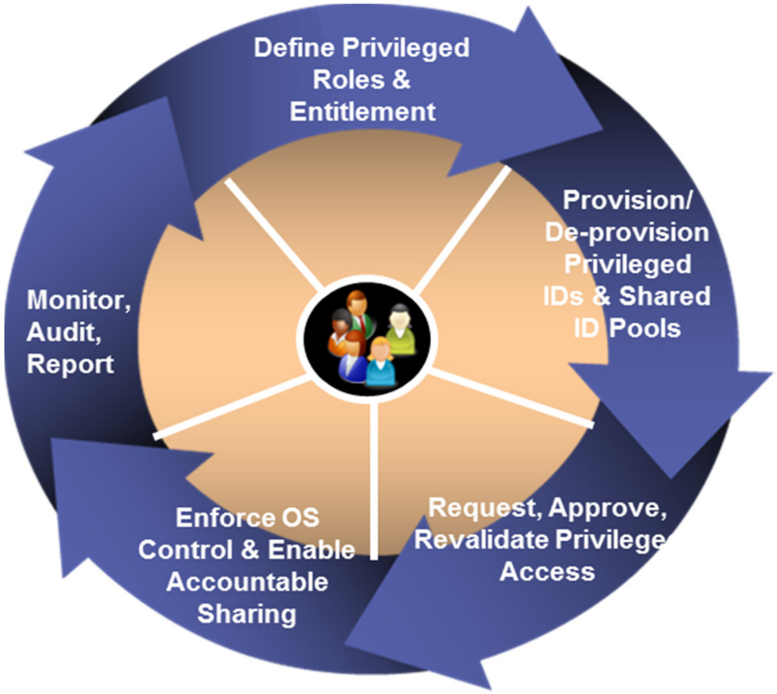
- Privileged user logs into eSSO
- eSSO automatically checks out/in shared ID as required to ensure accountability while simplifying usage

4

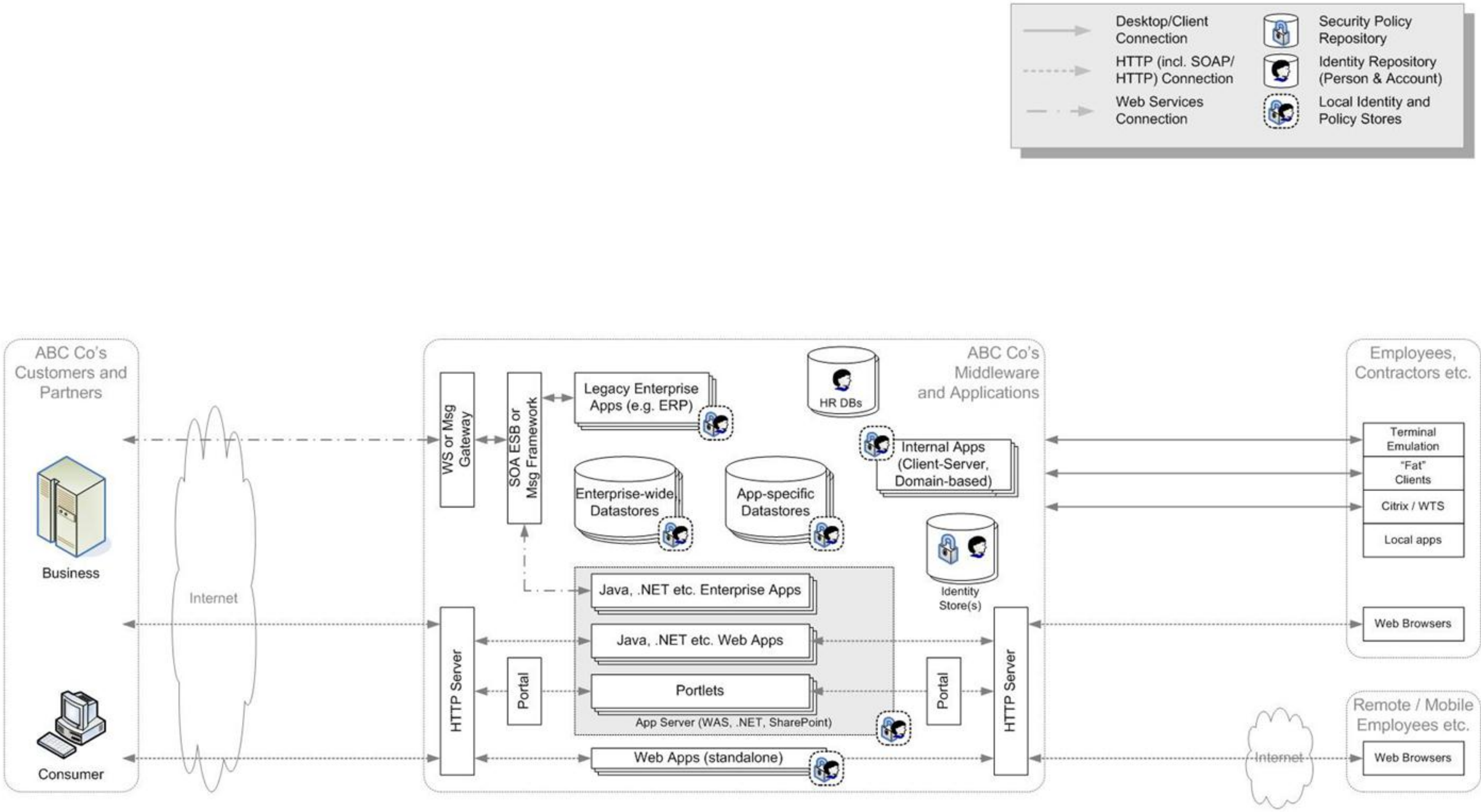
- SIEM monitors all logs for end to end tracking

Address the growing privileged ID problem with a complete life cycle solution

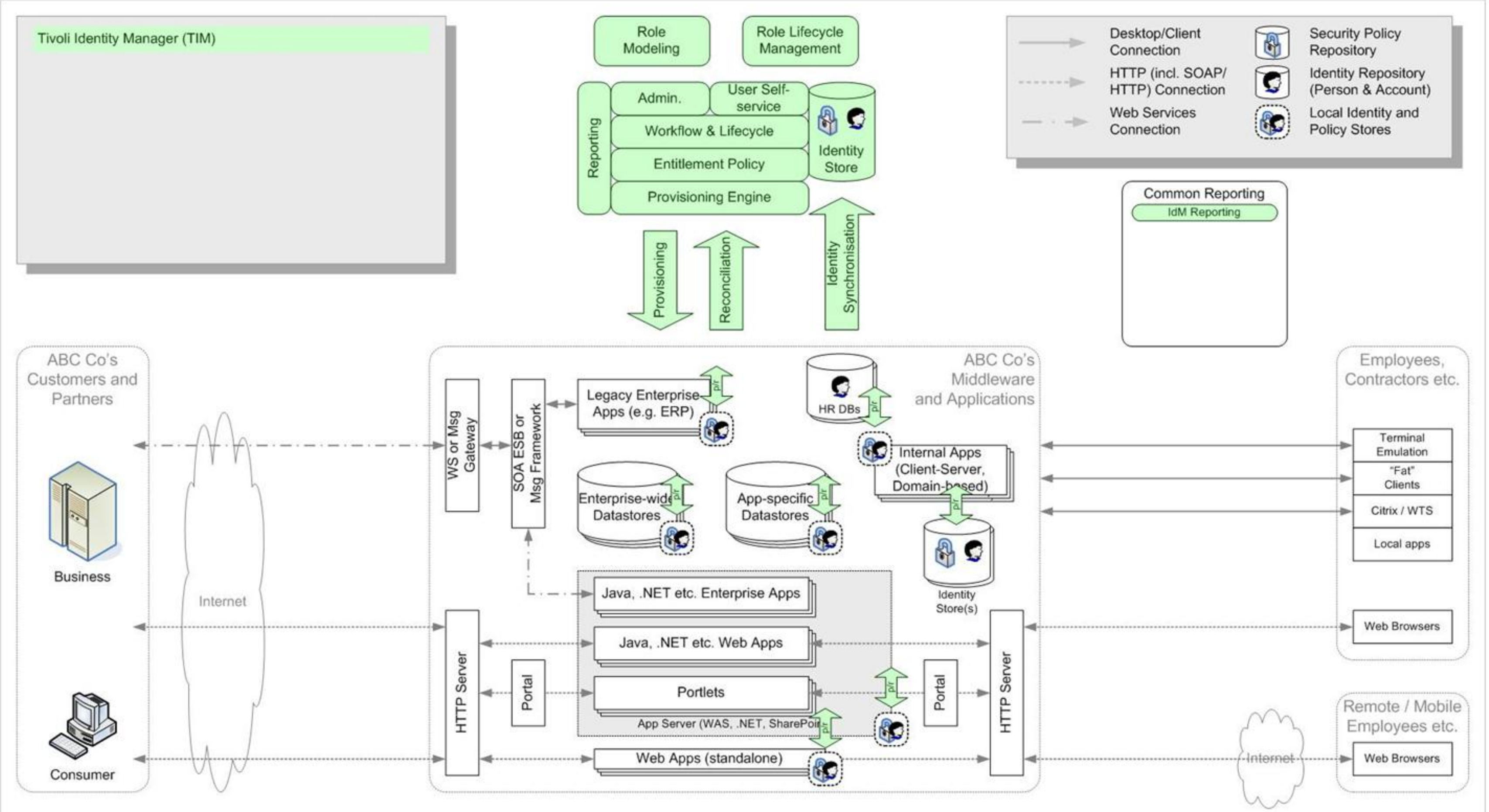
- Key trends are driving an exponential increase in Privileged IDs:
  - Virtualization is escalating the growth of Privileged IDs as these accounts are spread across multiple VMs
  - Data center consolidation creates a huge demand for privileged IDs as a large number of admins manage an ever growing number of servers
  - Cloud computing and the dynamic infrastructure is driving the growth of virtualization and data centers, further driving the exponential growth
- Benefits
  - Centralized Privileged ID management improves IT control and **reduces risk**
  - Automated sign on and check-in/out simplifies usage and **reduces cost**
  - Comprehensive tracking and reporting **enhances accountability and compliance**


Define Privileged Roles & Entitlement
Provision/ De-provision Privileged IDs & Shared ID Pools
Request, Approve, Revalidate Privilege Access
Enforce OS Control & Enable Accountable Sharing
Monitor, Audit, Report

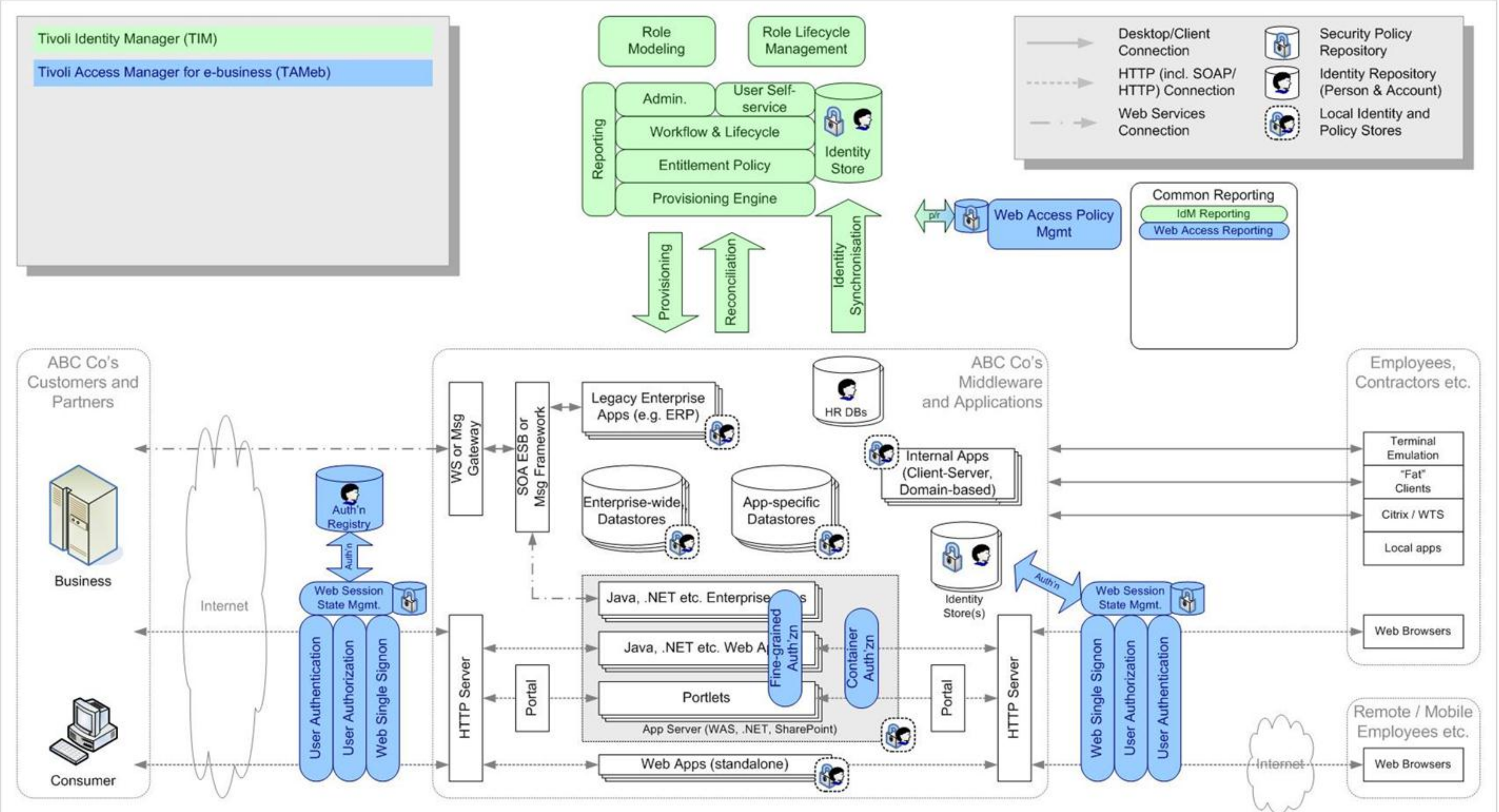
Generic Environment for Identity, Access and Compliance Management


Desktop/Client Connection
HTTP (incl. SOAP/ HTTP) Connection
Web Services Connection
Security Policy Repository
Identity Repository (Person & Account)
Local Identity and Policy Stores
ABC Co's Customers and Partners
Business
Consumer
Internet
ABC Co's Middleware and Applications
WS or Msg Gateway
SOA ESB or Msg Framework
Legacy Enterprise Apps (e.g. ERP)
HR DBs
Internal Apps (Client-Server, Domain-based)
Enterprise-wide Datastores
App-specific Datastores
Identity Store(s)
Java, .NET etc. Enterprise Apps
Java, .NET etc. Web Apps
Portlets
App Server (WAS, .NET, SharePoint)
Web Apps (standalone)
HTTP Server
Portal
Portal
HTTP Server
Employees, Contractors etc.
Terminal Emulation
"Fat" Clients
Citrix / WTS
Local apps
Web Browsers
Remote / Mobile Employees etc.
Internet
Web Browsers

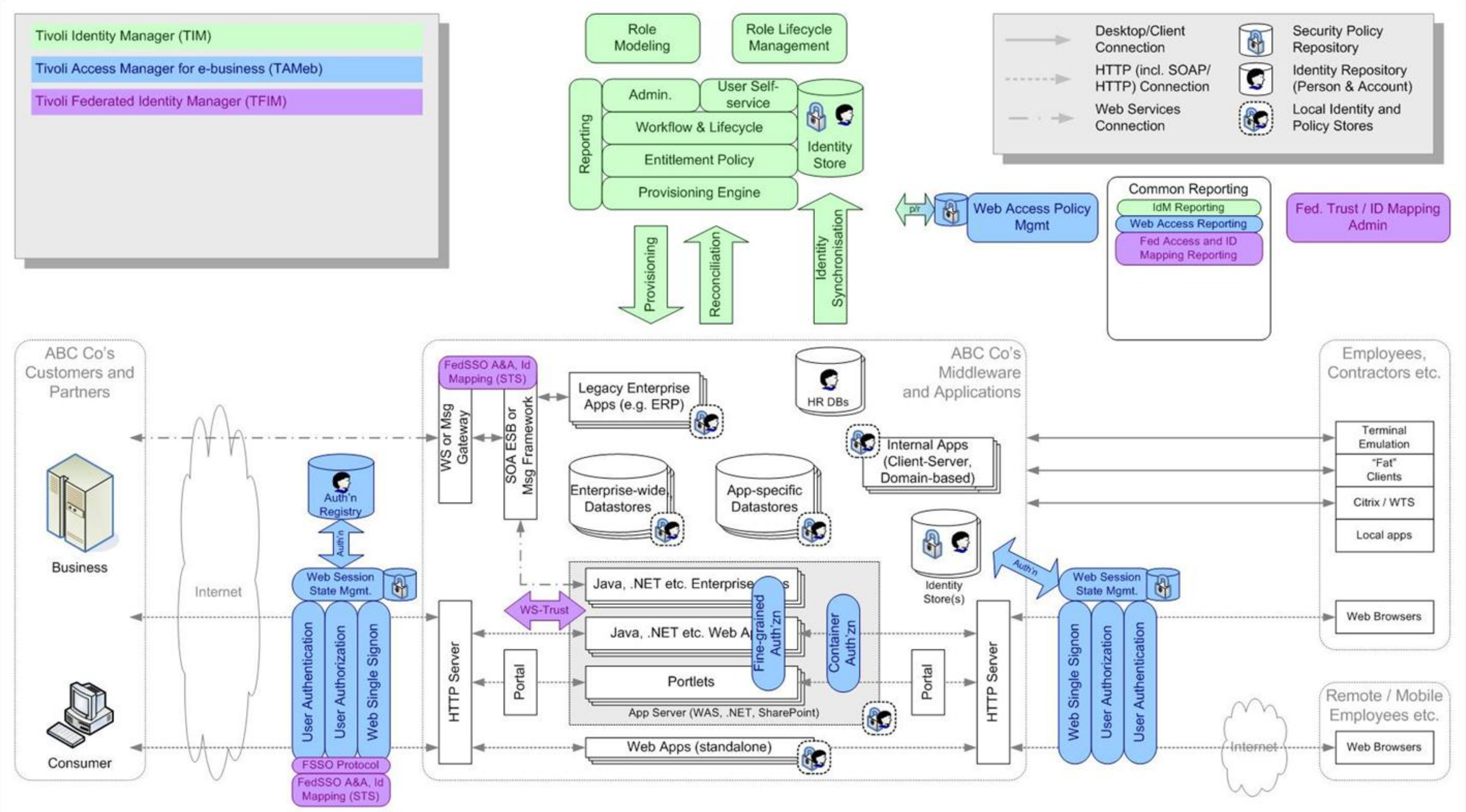
Identity Management



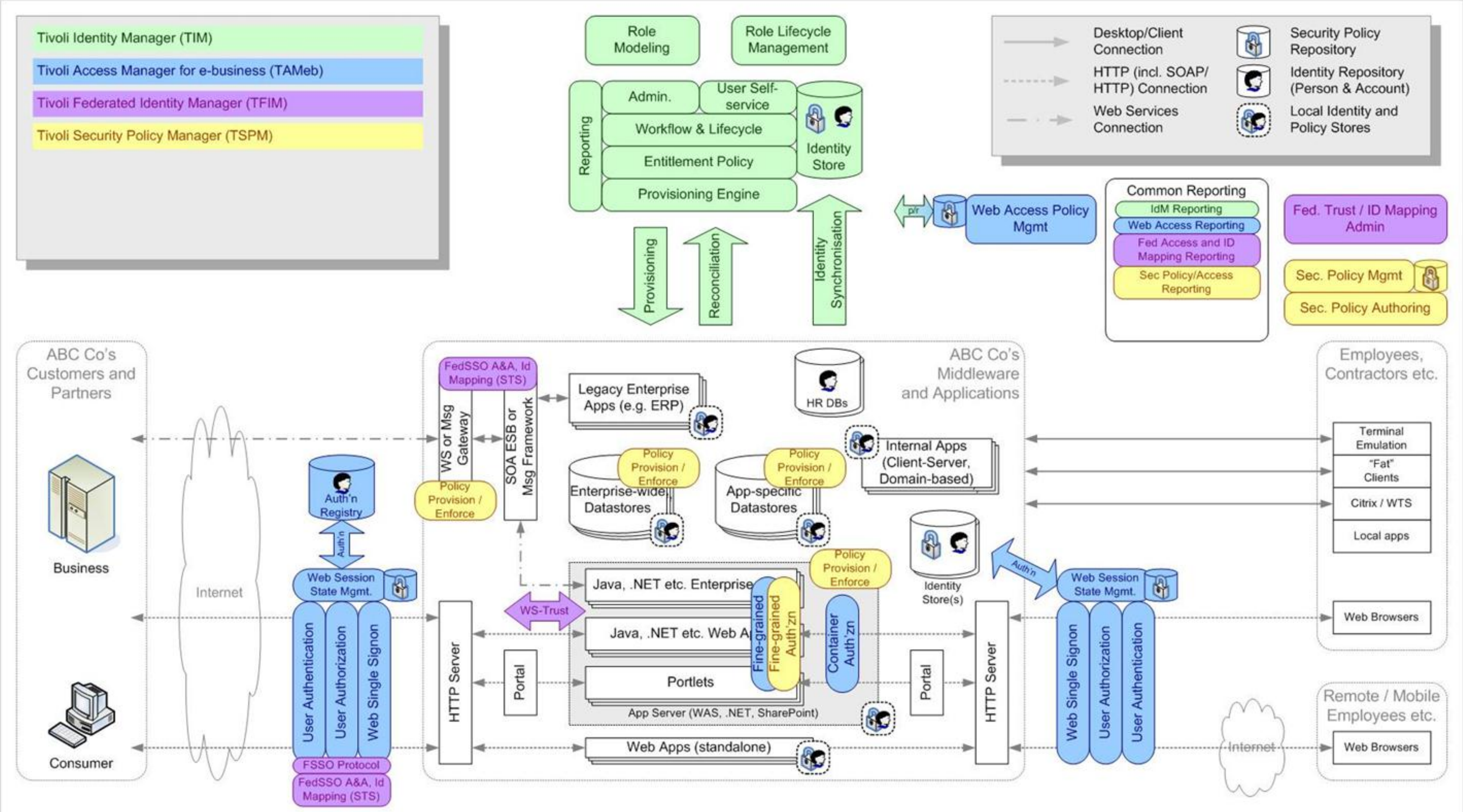
Web Access Control



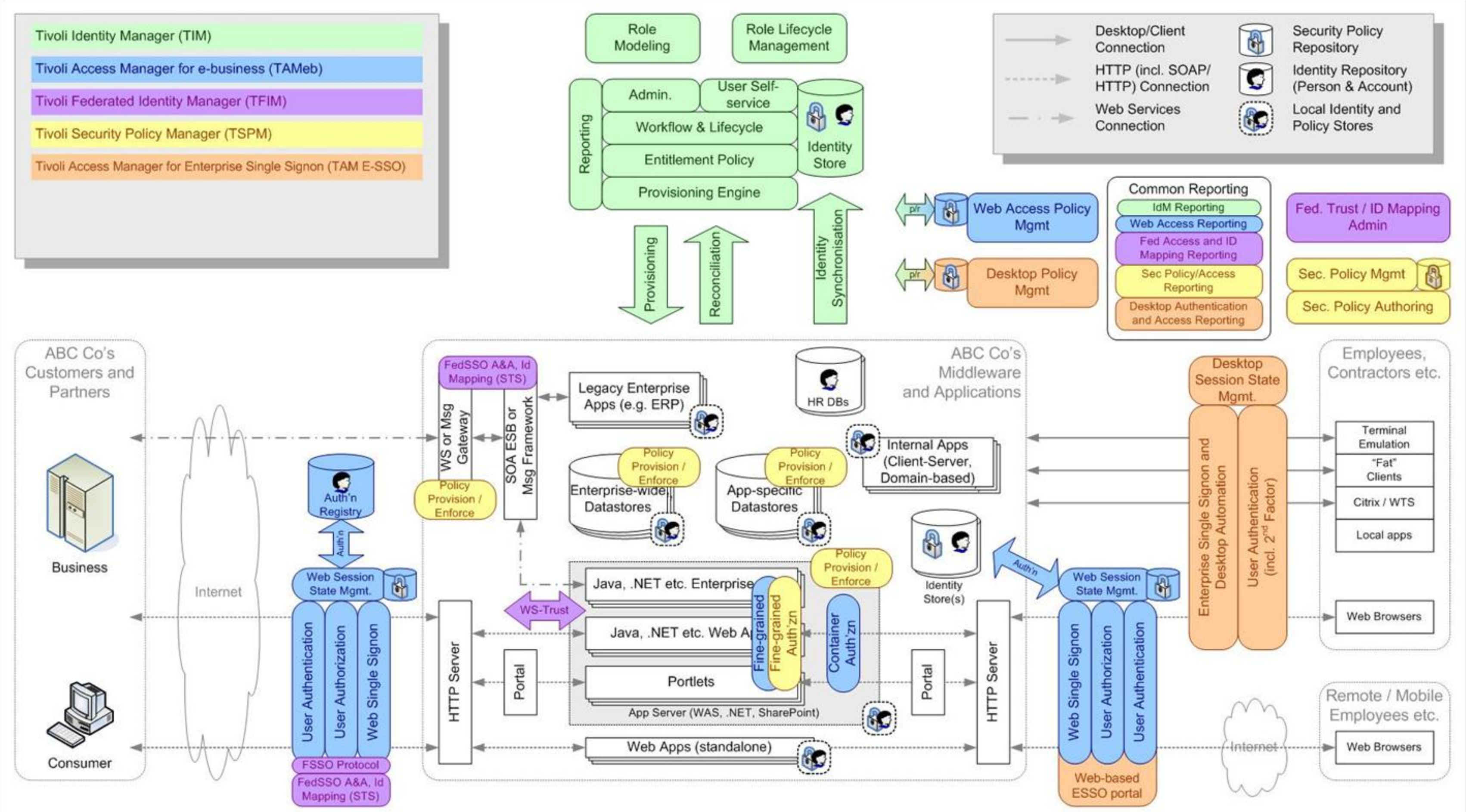
Federated Identity Management



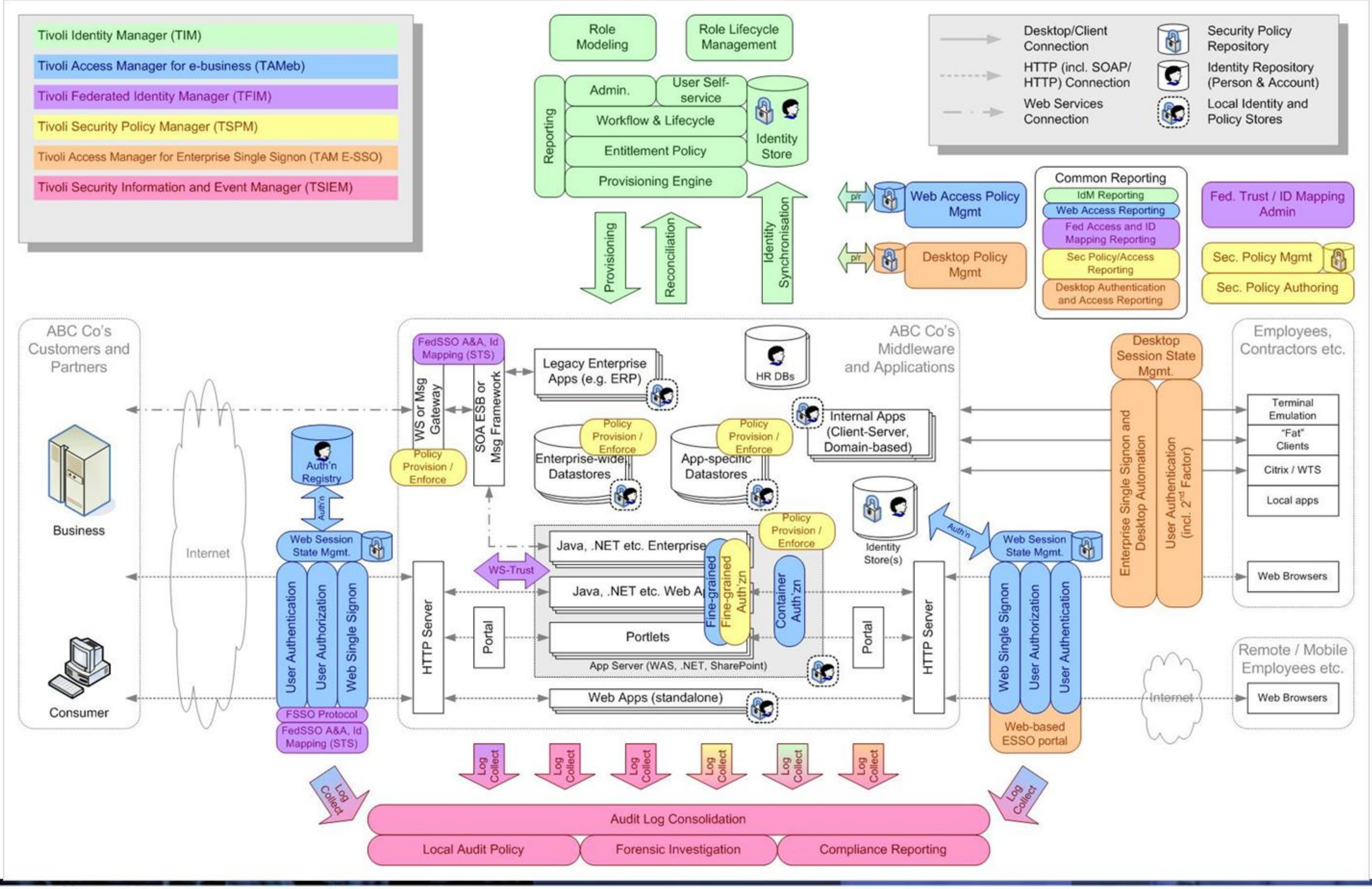
Security Policy Management


Tivoli Identity Manager (TIM)
Tivoli Access Manager for e-business (TAMeb)
Tivoli Federated Identity Manager (TFIM)
Tivoli Security Policy Manager (TSPM)
Role Modeling
Role Lifecycle Management
Reporting
Admin.
User Self-service
Workflow & Lifecycle
Entitlement Policy
Provisioning Engine
Identity Store
Provisioning
Reconciliation
Identity Synchronisation
Desktop/Client Connection
HTTP (incl. SOAP/ HTTP) Connection
Web Services Connection
Security Policy Repository
Identity Repository (Person & Account)
Local Identity and Policy Stores
p/r
Web Access Policy Mgmt
Common Reporting
IdM Reporting
Web Access Reporting
Fed Access and ID Mapping Reporting
Sec Policy/Access Reporting
Fed. Trust / ID Mapping Admin
Sec. Policy Mgmt
Sec. Policy Authoring
ABC Co's Customers and Partners
Business
Consumer
Internet
Auth'n Registry
Auth'n
Web Session State Mgmt.
User Authentication
User Authorization
Web Single Signon
FSSO Protocol
FedSSO A&A, Id Mapping (STS)
FedSSO A&A, Id Mapping (STS)
WS or Msg Gateway
Policy Provision / Enforce
SOA ESB or Msg Framework
Legacy Enterprise Apps (e.g. ERP)
HR DBs
ABC Co's Middleware and Applications
Enterprise-wide Datastores
Policy Provision / Enforce
App-specific Datastores
Policy Provision / Enforce
Internal Apps (Client-Server, Domain-based)
Identity Store(s)
Policy Provision / Enforce
WS-Trust
HTTP Server
Portal
Java, .NET etc. Enterprise
Java, .NET etc. Web Ap
Portlets
Fine-grained
Fine-grained Auth'zn
Container Auth'zn
App Server (WAS, .NET, SharePoint)
Web Apps (standalone)
Portal
HTTP Server
Auth'n
Web Session State Mgmt.
Web Single Signon
User Authorization
User Authentication
Employees, Contractors etc.
Terminal Emulation
"Fat" Clients
Citrix / WTS
Local apps
Web Browsers
Remote / Mobile Employees etc.
Internet
Web Browsers

Enterprise (Desktop) Single Signon


Tivoli Identity Manager (TIM)
Tivoli Access Manager for e-business (TAMeb)
Tivoli Federated Identity Manager (TFIM)
Tivoli Security Policy Manager (TSPM)
Tivoli Access Manager for Enterprise Single Signon (TAM E-SSO)
Role Modeling
Role Lifecycle Management
Reporting
Admin.
User Self-service
Workflow & Lifecycle
Entitlement Policy
Provisioning Engine
Identity Store
Provisioning
Reconciliation
Identity Synchronisation
Desktop/Client Connection
HTTP (incl. SOAP/ HTTP) Connection
Web Services Connection
Security Policy Repository
Identity Repository (Person & Account)
Local Identity and Policy Stores
p/r
Web Access Policy Mgmt
p/r
Desktop Policy Mgmt
Common Reporting
IdM Reporting
Web Access Reporting
Fed Access and ID Mapping Reporting
Sec Policy/Access Reporting
Desktop Authentication and Access Reporting
Fed. Trust / ID Mapping Admin
Sec. Policy Mgmt
Sec. Policy Authoring
ABC Co's Customers and Partners
Business
Consumer
Internet
Auth'n Registry
Auth'n
Web Session State Mgmt.
User Authentication
User Authorization
Web Single Signon
FSSO Protocol
FedSSO A&A, Id Mapping (STS)
FedSSO A&A, Id Mapping (STS)
WS or Msg Gateway
SOA ESB or Msg Framework
Policy Provision / Enforce
HTTP Server
Portal
WS-Trust
Legacy Enterprise Apps (e.g. ERP)
HR DBs
ABC Co's Middleware and Applications
Policy Provision / Enforce
Enterprise-wide Datastores
Policy Provision / Enforce
App-specific Datastores
Internal Apps (Client-Server, Domain-based)
Identity Store(s)
Policy Provision / Enforce
Java, .NET etc. Enterprise
Java, .NET etc. Web Ap
Portlets
Fine-grained
Fine-grained Auth'zn
Container Auth'zn
App Server (WAS, .NET, SharePoint)
Web Apps (standalone)
Portal
HTTP Server
Auth'n
Web Session State Mgmt.
Web Single Signon
User Authorization
User Authentication
Web-based ESSO portal
Desktop Session State Mgmt.
Enterprise Single Signon and Desktop Automation
User Authentication (incl. 2nd Factor)
Employees, Contractors etc.
Terminal Emulation
"Fat" Clients
Citrix / WTS
Local apps
Web Browsers
Internet
Remote / Mobile Employees etc.
Web Browsers

Audit Log Centralisation and Compliance Management



Tivoli Identity Manager (TIM)
Tivoli Access Manager for e-business (TAMeb)
Tivoli Federated Identity Manager (TFIM)
Tivoli Security Policy Manager (TSPM)
Tivoli Access Manager for Enterprise Single Signon (TAM E-SSO)
Tivoli Security Information and Event Manager (TSIEM)

Role Modeling
Role Lifecycle Management
Reporting
Admin.
User Self-service
Workflow & Lifecycle
Entitlement Policy
Provisioning Engine
Identity Store
Provisioning
Reconciliation
Identity Synchronisation

Desktop/Client Connection
HTTP (incl. SOAP/ HTTP) Connection
Web Services Connection
Security Policy Repository
Identity Repository (Person & Account)
Local Identity and Policy Stores

p/r
Web Access Policy Mgmt
p/r
Desktop Policy Mgmt

Common Reporting
IdM Reporting
Web Access Reporting
Fed Access and ID Mapping Reporting
Sec Policy/Access Reporting
Desktop Authentication and Access Reporting

Fed. Trust / ID Mapping Admin
Sec. Policy Mgmt
Sec. Policy Authoring

ABC Co's Customers and Partners
Business
Consumer
Internet

Auth'n Registry
Auth'n
Web Session State Mgmt.
User Authentication
User Authorization
Web Single Signon
FSSO Protocol
FedSSO A&A, Id Mapping (STS)

FedSSO A&A, Id Mapping (STS)
WS or Msg Gateway
SOA ESB or Msg Framework
Policy Provision / Enforce
Legacy Enterprise Apps (e.g. ERP)
HR DBs
ABC Co's Middleware and Applications
Policy Provision / Enforce
Enterprise-wide Datastores
Policy Provision / Enforce
App-specific Datastores
Internal Apps (Client-Server, Domain-based)
Identity Store(s)
Auth'n
Policy Provision / Enforce
WS-Trust
Java, .NET etc. Enterprise
Java, .NET etc. Web Ap
Portlets
Fine-grained
Fine-grained Auth'zn
Container Auth'zn
App Server (WAS, .NET, SharePoint)
Web Apps (standalone)
HTTP Server
Portal
Portal
HTTP Server

Web Session State Mgmt.
Web Single Signon
User Authorization
User Authentication
Web-based ESSO portal

Desktop Session State Mgmt.
Enterprise Single Signon and Desktop Automation
User Authentication (incl. 2nd Factor)

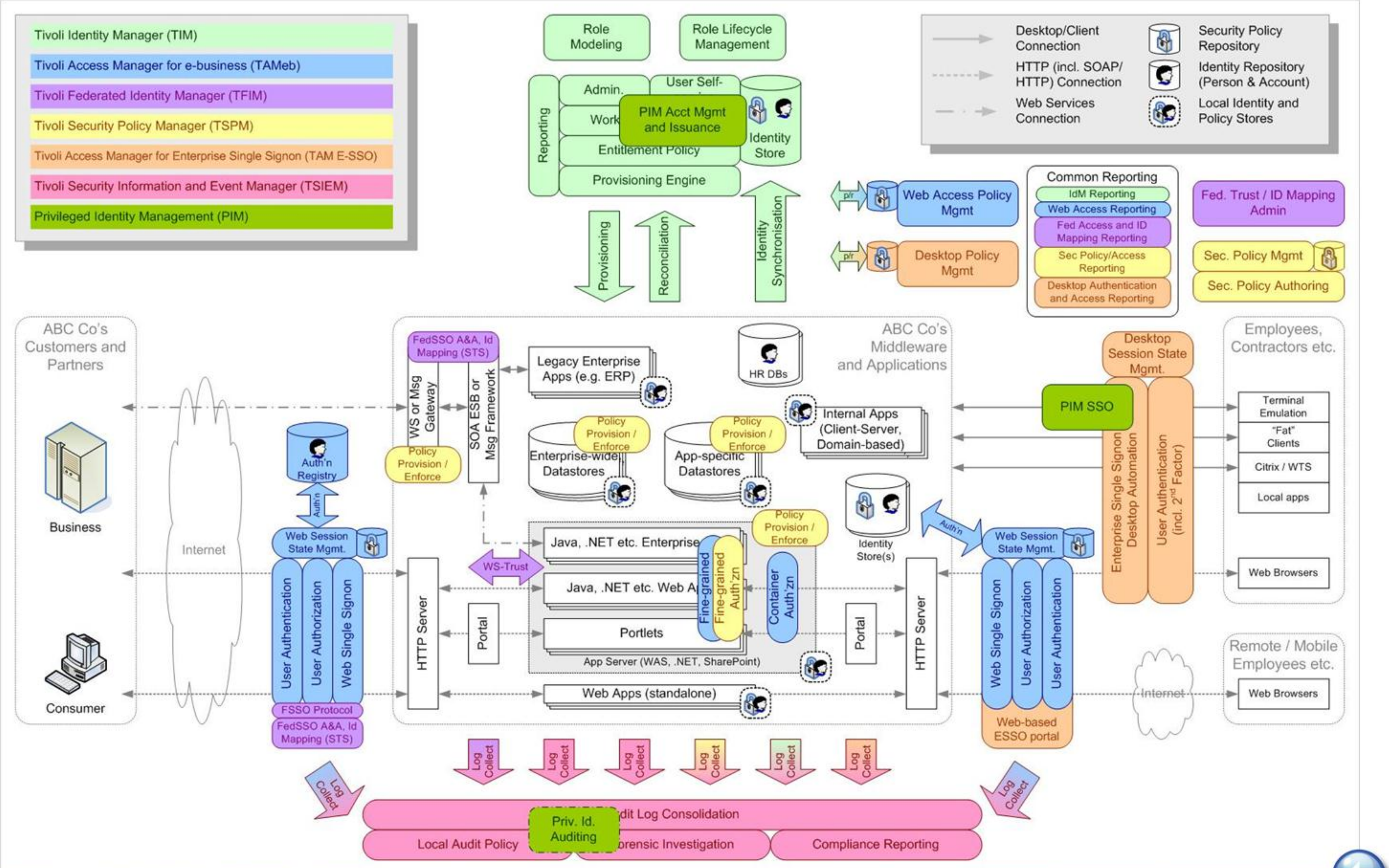
Employees, Contractors etc.
Terminal Emulation
"Fat" Clients
Citrix / WTS
Local apps
Web Browsers

Remote / Mobile Employees etc.
Internet
Web Browsers

Log Collect
Log Collect
Log Collect
Log Collect
Log Collect
Log Collect
Log Collect
Log Collect

Audit Log Consolidation
Local Audit Policy
Forensic Investigation
Compliance Reporting

Privileged Identity Management



Tivoli Identity Manager (TIM)
Tivoli Access Manager for e-business (TAMeb)
Tivoli Federated Identity Manager (TFIM)
Tivoli Security Policy Manager (TSPM)
Tivoli Access Manager for Enterprise Single Signon (TAM E-SSO)
Tivoli Security Information and Event Manager (TSIEM)
Privileged Identity Management (PIM)

Role Modeling
Role Lifecycle Management
Reporting
Admin.
User Self-
Work
PIM Acct Mgmt and Issuance
Entitlement Policy
Provisioning Engine
Identity Store
Provisioning
Reconciliation
Identity Synchronisation

Desktop/Client Connection
HTTP (incl. SOAP/ HTTP) Connection
Web Services Connection
Security Policy Repository
Identity Repository (Person & Account)
Local Identity and Policy Stores

p/r
Web Access Policy Mgmt
p/r
Desktop Policy Mgmt

Common Reporting
IdM Reporting
Web Access Reporting
Fed Access and ID Mapping Reporting
Sec Policy/Access Reporting
Desktop Authentication and Access Reporting

Fed. Trust / ID Mapping Admin
Sec. Policy Mgmt
Sec. Policy Authoring

ABC Co's Customers and Partners
Business
Consumer
Internet

Auth'n Registry
Auth'n
Web Session State Mgmt.
User Authentication
User Authorization
Web Single Signon
FSSO Protocol
FedSSO A&A, Id Mapping (STS)

ABC Co's Middleware and Applications
FedSSO A&A, Id Mapping (STS)
WS or Msg Gateway
SOA ESB or Msg Framework
Policy Provision / Enforce
Legacy Enterprise Apps (e.g. ERP)
HR DBs
Internal Apps (Client-Server, Domain-based)
Policy Provision / Enforce
Enterprise-wide Datastores
Policy Provision / Enforce
App-specific Datastores
Identity Store(s)
Policy Provision / Enforce
WS-Trust
Java, .NET etc. Enterprise
Java, .NET etc. Web A
Portlets
Fine-grained
Fine-grained Auth'zn
Container Auth'zn
App Server (WAS, .NET, SharePoint)
Web Apps (standalone)
HTTP Server
Portal
Portal
HTTP Server
Auth'n

Web Session State Mgmt.
Web Single Signon
User Authorization
User Authentication
Web-based ESSO portal

Desktop Session State Mgmt.
PIM SSO
Enterprise Single Signon Desktop Automation
User Authentication (incl. 2nd Factor)

Employees, Contractors etc.
Terminal Emulation
"Fat" Clients
Citrix / WTS
Local apps
Web Browsers

Remote / Mobile Employees etc.
Internet
Web Browsers

Log Collect
Log Collect
Log Collect
Log Collect
Log Collect
Log Collect
Log Collect
Log Collect

Priv. Id. Auditing
dit Log Consolidation
Local Audit Policy
orensic Investigation
Compliance Reporting

Resources

- www.ibm.com/security
- IBM Redguide: Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

Thank
You